ABSTRACT OF THE DISCLOSURE

A key agreement protocol for preventing key-share attacks wherein a method is provided for establishing a common shared key between a pair of correspondents in a station-to-station protocol by exchanging messages between the correspondents and including identification information in said messages, the information being identifiable to one or other of said correspondents to thereby establish said common key.